UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/562,488	12/22/2005	Adrian Alvarez Diez	DE920030032US1	6307

30206 7590 11/14/2008

IBM CORPORATION
ROCHESTER IP LAW DEPT. 917
3605 HIGHWAY 52 NORTH
ROCHESTER, MN 55901-7829

EXAMINER	
SHAW, PETER C	

ART UNIT	PAPER NUMBER
4143	

MAIL DATE	DELIVERY MODE
11/14/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/562,488	DIEZ ET AL.	
	Examiner	Art Unit	
	PETER SHAW	4143	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *22 December 2005*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-17* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-17* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *22 December 2005* is/are: a)☐ accepted or b)☒ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *03/22/2006*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-17 are pending in this action.

Drawings

2. The drawings are objected to as failing to comply with 37 CFR 1.84(p)(4) because reference character "2" has been used to designate both "n-server application" and "server application." Corrected drawing sheets in compliance with 37 CFR 1.121(d) are required in reply to the Office action to avoid abandonment of the application. Any amended replacement drawing sheet should include all of the figures appearing on the immediate prior version of the sheet, even if only one figure is being amended. Each drawing sheet submitted after the filing date of an application must be labeled in the top margin as either "Replacement Sheet" or "New Sheet" pursuant to 37 CFR 1.121(d). If the changes are not accepted by the examiner, the applicant will be notified and informed of any required corrective action in the next Office action. The objection to the drawings will not be held in abeyance.

Specification

3. The use of the trademark IBM has been noted in this application. It should be capitalized wherever it appears and be accompanied by the generic terminology.

Although the use of trademarks is permissible in patent applications, the proprietary nature of the marks should be respected and every effort made to prevent their use in any manner which might adversely affect their validity as trademarks.

Claim Objections

4. Claim 16, line 29, it is suggested that "a Certificate verifier component" be amended to "a certificate verifier component."

Lack of Antecedent Basis

5. Claim 10 recites the limitation "said each server" in line 3. There is insufficient antecedent basis for this limitation in the claim. It is suggested that the limitation be amended to "each server" or that it be defined earlier in the claim.

6. Claim 14 recites the limitation "said different fingerprints" in line 1. There is insufficient antecedent basis for this limitation in the claim. It is suggested that the limitation be amended to "said two different fingerprints."

7. Claim 16 recites the limitation "said common data store" in line 36. There is insufficient antecedent basis for this limitation in the claim. It is suggested that the limitation be amended to "a common data store" or that it be defined earlier in the claim.

8. Claim 17 recites the limitation "the computer" in line 4. There is insufficient antecedent basis for this limitation in the claim. It is suggested that the limitation be amended to "a computer" or that it be defined earlier in the claim.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

9. Claim 1, 2, 4, 5, 7, 8, 9, 12 and 16 are rejected under 35 U.S.C. 112, second paragraph, for failing to particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

As per claims 1, 4, 5, 7, 8, and 9, the limitations "third tier server certificates," "third tier certificate," "original third tier certificate," and "received third tier certificate" are recited. It is unclear whether these limitations refer to the same component of the invention or different ones. It is suggested that descriptors be used in each limitation to clearly differentiate between different components.

As per claims 1, 2, 4, and 5, the limitations "all necessary information," "necessary information," and "information" are used to refer to the same component of the invention. It is suggested that one name be chosen and consistently used.

As per claims 7, 12, and 16, the limitations "third tier server," "third tier server system," and "server system" are recited. It is unclear whether these limitations refer to the same component of the invention or different ones. It is suggested that one name be chosen for each limitation and consistently used.

Claim Rejections - 35 USC § 101

35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

10. Claims 12-16 are rejected under 35 U.S.C. 101 because the claimed inventions are directed to non-statutory subject matter. Claims 12-17 are considered functional descriptive material because the server and client components have not been limited to hardware in the specification.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

11. Claims 1, 4-9, and 16-17 are rejected under 35 U.S.C. 103(a) as being unpatentable over Xiao (US PGPUB No. 2002/0152382) [as cited in Information Disclosure Statement] in view of Applicant's Admitted Prior Art [hereinafter "AAPA"].

As per claim 1, Xiao teaches a method for validating and verifying a certificate by a client comprising: (1) receiving, from a common database of a client system ([0088],

lines 2-3, "A TIO stored on a trusted server" and "a common database" serve the same function; both store certificates and other authentication information of already validated certificates for verifying later received certificates.), the necessary information to accept or decline a connection from a server ([0063], lines 3-5, the hash value of trusted certificates, i.e. thumbprint or fingerprint); (2) comparing, the necessary information received from the common database of the client system (Fig. 2, 106, comparing thumbprints), with authentication data, i.e. certificate, received from the server (Fig. 2, 102); and (3) accepting/authenticating server if the necessary information matches the authentication data (Fig. 2, 108, matched thumbprints; Fig. 2, 116, leads to authenticated server).

Xiao does not teach validating a certificate by a client and later verifying the certificate by servers running the same application as the client. AAPA teaches validating a certificate by a client ([0013], lines 9-10, Manual accept/reject is viewed to represent any form of validation that is more costly than verification.) and later verifying the certificate by servers running the same application as the client ([0013], lines 18-19). At the time of invention, it would have been obvious to one of ordinary skill in the art, to combine the teachings of Xiao, with the teachings of AAPA, validating a certificate by a client and later verifying the certificate by servers running the same application as the client, to improve efficiency by limiting the amount of validation required.

As per claim 4, the combination of Xiao and AAPA teaches the necessary information to be a certificate stored in the common database (Xiao, [0076], line 4, "A certified

thumbprint" is all that is necessary to verify a received certificate.), along with the name of the server which originally transmitted the certificate (Xiao, [0098], lines 24-25, "Associated trust information" is viewed to include server name; also, it is well known in the art that a certificate, hashed or not, contains the "subject" server name.).

As per claim 5, the combination of Xiao and AAPA teaches the necessary information to be a fingerprint of a certificate stored in the common database (Xiao, [0076], line 4, "certificate thumbprint"), along with the name of the server which originally transmitted the certificate (Xiao, [0098], lines 24-25, "Associated trust information" is viewed to include server name; also, it is well known in the art that a certificate, hashed or not, contains the "subject" server name.).

As per claim 6, the combination of Xiao and AAPA teaches the necessary information to be one fingerprint of a certificate stored in the common database (Xiao, [0076], line 4, "certificate thumbprint") along with the name of the server which originally transmitted the certificate and the certificate name (Xiao, [0098], lines 24-25, "Associated trust information" is viewed to include server name and certificate name; also, it is well known in the art that a certificate, hashed or not, contains the "subject" server name and certificate name.).

The combination of Xiao and AAPA does not explicitly teach storing two different fingerprints of a certificate in a common database. However, the combination of Xiao implicitly discloses storing two different fingerprints (Xiao, [0076], line 4, storing one

fingerprint) of a certificate in a common database to increase security by performing the security measure twice.

As per claim 7, Xiao teaches a method comprising: (1) receiving a certificate from a server system (Fig. 2, 102); (2) determining whether the certificate is trustworthy, i.e. certificate validation (Fig. 2, 122, Validation performed by root retrieving certificate.); (3) storing certificate in a common database if trustworthy ([0078], line 7-8, Updating the TIO involves storing thumbprints of certificates in its table.); and (4) transferring all necessary information to accept or decline server ([0088], lines 2-3, The hash values in the TIO are all that are necessary to validate a certificate.).

Xiao does not teach validating a certificate by a client and later verifying the certificate by servers running the same application as the client. AAPA teaches validating a certificate by a client ([0013], lines 9-10, Manual accept/reject is viewed to represent any form of validation that is more costly than verification.) and later verifying the certificate by servers running the same application as the client ([0013], lines 18-19). At the time of invention, it would have been obvious to one of ordinary skill in the art, to combine the teachings of Xiao, with the teachings of AAPA, validating a certificate by a client and later verifying the certificate by servers running the same application as the client, to improve efficiency by limiting the amount of validation required.

As per claim 8, the combination of Xiao and AAPA teaches storing certificate in the common database (Xiao, [0076], line 4, "A certified thumbprint" is all that is necessary to

verify a received certificate.), along with the name of the server which originally transmitted the certificate (Xiao, [0098], lines 24-25, "Associated trust information" is viewed to include server name; also, it is well known in the art that a certificate, hashed or not, contains the "subject" server name.).

As per claim 9, the combination of Xiao and AAPA teaches receiving a certificate via a secure transmission protocol (Xiao, [0004], line 1).

As per claim 16, Xiao teaches a client system comprising: (1) a connection negotiator component, for receiving certificates, via a secure connection ([0088], lines 2-3, "A TIO stored on a trusted server" and "a common database" serve the same function; both store certificates and other authentication information of already validated certificates for verifying later received certificates.); (2) a common database, for storing certificates accepted as trustworthy ([0088], lines 2-3, "A TIO stored on a trusted server" and "a common database" serve the same function; both store certificates and other authentication information of already validated certificates for verifying later received certificates.); (3) a certificate verifier component, for comparing information in the common database with a received certificate (Fig. 2, 106, Hashing received certificate and comparing thumbprints.); (4) a user interface component, for accepting/rejecting certificates not found in common database (Fig. 2, 114, Failing handshake means rejecting certificate.); and (5) a certificate transmitter component, for extracting all necessary information from common database ([0076], lines 3-5, Database and TIO

serve the same function of holding trusted certificates in the form of hashed thumbprints) and sending it to a client ([0088], line 2, The authentication information can be sent by a trusted server to the client.).

Xiao does not teach validating a certificate by a client and later verifying the certificate by servers running the same application as the client. AAPA teaches validating a certificate by a client ([0013], lines 9-10, Manual accept/reject is viewed to represent any form of validation that is more costly than verification.) and later verifying the certificate by servers running the same application as the client ([0013], lines 18-19). At the time of invention, it would have been obvious to one of ordinary skill in the art, to combine the teachings of Xiao, with the teachings of AAPA, validating a certificate by a client and later verifying the certificate by servers running the same application as the client, to improve efficiency by limiting the amount of validation required.

As per claim 17, the combination of Xiao and AAPA does not teaches a computer program stored on internal memory of a digital computer containing software code to execute the method of claim 1. However, the combination of Xiao and AAPA implicitly teaches a computer program stored on internal memory of a digital computer containing software code to execute the method of claim 1 (Fig. 2, 108, matched thumbprints; Fig. 2, 116, leads to authenticated server).

12. Claims 2-3 and 10-15 are rejected under 35 U.S.C. 103(a) as being unpatentable over Xiao in view of AAPA and further in view of Ramasibramani et al. (US Patent No. 6,233,577) [hereinafter "Ramasubramani"].

As per claim 2, the combination of Xiao and AAPA does not teach receiving information via a non-continuous client-server connection, i.e. asynchronous. However, Ramasubramani teaches receiving information via a non-continuous client-server connection, i.e. asynchronous (Ramasubramani, Col. 7, line 64, "receiving/sending certificates"). At the time of invention, it would have been obvious to one of ordinary skill in the art, to combine the teachings of Xiao and AAPA, with the teachings of Ramasubramani, receiving information via a non-continuous client-server connection, i.e. asynchronous, to allow for more flexibility as to when authentication data is to be sent or received.

As per claim 3, the combination of Xiao, AAPA, and Ramasubramani teaches transmitting information via a secure transmission protocol (Xiao, [0004], line 1).

As per claim 10, the combination of Xiao and AAPA does not teach receiving information via a non-continuous client-server connection, i.e. asynchronous. However, Ramasubramani teaches receiving information via a non-continuous client-server connection, i.e. asynchronous (Ramasubramani, Col. 7, line 64, "receiving/sending certificates"). At the time of invention, it would have been obvious to one of ordinary

skill in the art, to combine the teachings of Xiao and AAPA, with the teachings of Ramasubramani, receiving information via a non-continuous client-server connection, i.e. asynchronous, to allow for more flexibility as to when authentication data is to be sent or received.

As per claim 11, the combination of Xiao, AAPA, and Ramasubramani teaches authenticating a client system via a user ID and/or password (Ramasubramani, Col. 7, lines 15-16).

As per claim 12, Xiao teaches a client system comprising: (1) a transfer server component, which supports a secure connection ([0004], line 1), for receiving all necessary information to verify a certificate ([0063], lines 3-5, the hash value of trusted certificates, i.e. thumbprint or fingerprint); (2) a connection negotiator component, which supports a secure connection ([0004], line 1), for receiving certificates (Fig. 2, 102); and (3) a certificate verifier component, for comparing all necessary information with a received certificate (Fig. 2, 106, comparing thumbprints).

Xiao does not teach validating a certificate by a client and later verifying the certificate by servers running the same application as the client. AAPA teaches validating a certificate by a client ([0013], lines 9-10, Manual accept/reject is viewed to represent any form of validation that is more costly than verification.) and later verifying the certificate by servers running the same application as the client ([0013], lines 18-19). At the time of invention, it would have been obvious to one of ordinary skill in the art, to

combine the teachings of Xiao, with the teachings of AAPA, validating a certificate by a client and later verifying the certificate by servers running the same application as the client, to improve efficiency by limiting the amount of validation required.

The combination of Xiao and AAPA does not teach a non-continuous connection, i.e. asynchronous. Ramasubramani teaches a non-continuous connection, i.e. asynchronous (Col. 7, line 64, "receiving/sending certificates"). At the time of invention, it would have been obvious to one of ordinary skill in the art to combine the teachings of Xiao and AAPA, with the teachings of Ramasubramani, a non-continuous connection, i.e. asynchronous, to allow for more flexibility as to when authentication data is to be sent or received.

As per claim 13, the combination of Xiao, AAPA, and Ramasubramani teaches the necessary information to be one fingerprint of a certificate stored in the common database (Xiao, [0076], line 4, "certificate thumbprint"), along with the name of the server which originally transmitted the certificate and the certificate name (Xiao, [0098], lines 24-25, "Associated trust information" is viewed to include server name and certificate name; also, it is well known in the art that a certificate, hashed or not, contains the "subject" server name and certificate name.).

The combination of Xiao, AAPA, and Ramasubramani does not explicitly teach storing two different fingerprints of a certificate in a common database. However, the combination of Xiao, AAPA, and Ramasubramani implicitly discloses storing two

different fingerprints of a certificate in a common database (Xiao, [0076], line 4, storing one fingerprint) to increase security by performing the security measure twice.

As per claim 14, the combination of Xiao, AAPA, and Ramasubramani teaches applying one algorithm to a certificate to generate one fingerprint (Xiao, [0098]. line 15 and 34).

The combination of Xiao, AAPA, and Ramasubramani does not explicitly teach applying two different algorithms to a certificate to generate two different fingerprints. However, the combination of Xiao, AAPA, and Ramasubramani implicitly discloses applying two different algorithms to a certificate to generate two different fingerprints (Xiao, [0098]. line 15 and 34, one algorithm, one fingerprint), to increase security by performing the security measure twice.

As per claim 15, the combination of Xiao, AAPA, and Ramasubramani teaches one algorithm in the server system (Xiao, [0098]. line 15 and 34).
The combination of Xiao, AAPA, and Ramasubramani does not explicitly teach two algorithms in the server system. However, the combination of Xiao, AAPA, and Ramasubramani implicitly discloses two algorithms in the server system (Xiao, [0098]. line 15 and 34, one algorithm in server system), to increase security by performing the security measure twice.

Conclusion

13. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. Koehler (US Patent No. 6,301,658) describes a common database used for verification purposes along with initial certificate validation.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to PETER SHAW whose telephone number is (571)270-7179. The examiner can normally be reached on Monday - Friday 7:30 A.M. to 5:00 P.M.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, NABIL EL-HADY can be reached on (571) 272-3963. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/PETER SHAW/
Examiner, Art Unit 4143

November 6, 2008

/NABIL EL-HADY/
Supervisory Patent Examiner, Art Unit 4143